## Trading privacy for security

van den Hoven van Genderen, R.

***published in***
Amsterdam Law Forum
2009

***document version***
Publisher's PDF, also known as Version of record



***citation for published version (APA)***
van den Hoven van Genderen, R. (2009). Trading privacy for security. *Amsterdam Law Forum*, *1*(4).

amsterdamlawforum
VU University Amsterdam

# TRADING PRIVACY FOR SECURITY

*Rob van den Hoven van Genderen*[*]

> "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement" (William Pitt, English Parliamentarian, 1765).

## Introduction

Privacy is one of the most personal human rights, for it includes all aspects of personal life and behaviour. In our current information society this personal information is used by private and public parties as a 'natural resource' for commercial and public policy activities. Certainly in the areas with perceived 'threats to society', authorities seem to have little hesitance to use this personal information. Under most circumstances the privacy right of the individual is considered to be outweighed by the general interest. But even the data-subjects themselves do think that privacy is of less importance than protection against perceived terrorist threats.

The concept of private property seems to be the source of all integrity of private possessions, including the inviolability of body and soul. Locke stated that the state's only reason of existence was its function to protect life, liberty and estate, and would only be justified if this purpose could be fulfilled. According to the International Court of Justice,

> "the jurisdiction of a State is exclusive within the limits fixed by international law – using this expression in its wider sense, that is to say, embracing both customary law and general as well as particular treaty law".[1]

Therefore, State sovereignty must be interpreted in view of, and combined with, general principles of international law such as the general prohibition of abuses of rights, proportionality, respect of other States' sovereignty, due diligence, 'minimum standards of civilisation', *et cetera*.[2] Although these principles are considered to form the basis of any national or international

---

[*] *Rob van den Hoven van Genderen is associate professor at the Computer Law Institute of the Law Faculty of the VU, Amsterdam. He has published articles and books on IT and law and has been chairman of the Netherlands Informatics and Law Association for more ten years. Further he has been board member in the telecommunication industry and is advisor for the Council of Europe, United Nations and the Nato Scientific Council on this issue. He is also advisor and associate to Switchlegal lawyers in Amsterdam.*

[1] PCIJ, Advisory Opinion, *Nationality Decrees Issued in Tunis and Morocco*, Series B, N° 4, p. 23; italics in the original text, underlining added.

[2] PCIJ, Advisory Opinion, *Nationality Decrees Issued in Tunis and Morocco*, Series B, N° 4, p. 24.

legal system, the actual application and definition has been a constant subject of discussion.[2]

In our changing society there is a tendency by governmental authorities to hold control over information and personal data streams, and to combine all informational sources to a single point of entrance. There is an increasing need to define limits to the use of personal data by national and international regulatory standards. In Article 8 of the European Convention on Human Rights (ECHR) it is stated that: "Everyone has the right to respect for his private and family life, his home and his correspondence." As the second paragraph indicates, this right is not absolute:

> "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Since the beginning of the 21st century, on the waves of (perceived) terrorism, the fundamental rights laid down in international treaties are often restricted. The international human rights treaties contain 'escape clauses' that allow sovereign states to restrict fundamental rights if there are justified circumstances to do so. These circumstances are ambiguous and are certainly not clearly defined in either national or international regulation. Article 8 of the ECHR is also applicable to actions of justice or the national security agencies, but who is controlling them?

## I. Extension of Data Processing by Authorities

We see an increasing adaptation of 'conventional' crime to cybercrime, including international terrorism because of the digitalisation, convergence of technologies and globalisation of Information and Communication Technology (ICT). Traditional measures of investigation by police and judicial authorities such as surveillance and tapping of electronic communication do not fit to these changes. Therefore special procedures need to be developed, such as 'data mining' and digitalised analysis of personal behaviour by profiling techniques. The criminal actors are using those techniques as well to commit their crimes and acts of terrorism, and thus we must be prepared to use similar means to combat the criminal actions.

---

[3] The municipal codes of well over a dozen countries expressly provide for the application of the general principles of law in the absence of specific legal provisions or of custom, and the Statute of the International Court of Justice stipulates that 'the general principles of law recognised by civilised nations' constitute one of the sources of international law to be applied by the Court; but the exact meaning and scope of this section of the Statute have always been a subject of controversy amongst international lawyers; see B. Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, London: University College 2006.

As stated in the explanatory report on the Convention on Cybercrime:

> "The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society." [4]

## II. Cybercrime

Due to the international nature of crimes as acts of terrorism, international co-ordinated investigations and the use of personal data must be made possible. However, a sharp eye must be kept on their limitations in the interest of human rights, and specifically the protection of the privacy of individuals which takes into account the evolution of data availability.

The key questions to confront are: how can the tension between privacy protection and criminal investigation and measures of protecting state security be resolved in an acceptable way, and what adaptations to the existing regulatory framework are needed?

The Cybercrime Convention[5] states that the actions of police and justice should be governed by restrictive measures based on the privacy concerns. Member States shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the relevant case law from the European Court of Justice, and national legislation and case law. The power or procedure shall be proportional to the nature and circumstances of the offence.

The question is how the nature and circumstances of the offence are weighed and by whom? What measures can be taken by governmental and police authorities to restrain this development in a way that will preserve existing privacy rights? To what extent are authorities free to use personal data and from what sources? There is publicly available data from the Internet and other public sources, but also data acquired in the execution of public tasks, often available in governmental databases. Are criminal investigators and security agencies allowed to use the data in the same or a more inquisitive way than other governmental authorities, and should exchange by

[4] Convention on Cybercrime 2001.
[5] Convention on Cybercrime 2001, explanatory report, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm ETS (accessed on 31 August 2009).

governmental agencies be allowed? Under what circumstances and to what extent should this be possible? Can laws be specified in such a way that the balance between different purposes in protection of privacy as a fundamental right on one hand, and the protection of state integrity as protector of national interest on the other, is preserved?

## III. Terrorist Threats as Lever for Increasing Competences for the National Intelligence Agency

The European Convention on Prevention of Terrorism states in Article 12:

> "Each Party shall ensure that the establishment, implementation and application of the criminalisation under Articles 5 to 7 and 9 of this Convention are carried out while respecting human rights obligations, in particular the right to freedom of expression, freedom of association and freedom of religion, as set forth in, where applicable to that Party, the Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other obligations under international law."[6]

It is striking and illustrative that privacy is not listed as one of the human rights that can limit actions against terrorism.

An interesting example can be found in the Dutch government report on information for the national intelligence agencies: Data for Decisiveness (*data voor daadkracht*) citing a Dutch poet from the early 19th century: "Although we do not know the reason, it probably has been a good one".[7] This was a means of indicating that we are expected to place our trust in the government, whatever they are doing with our personal data. According to this report, the enormous growth of databases and communication media, as well as the development of advanced technology to search, gives ample opportunity to intelligence agencies to realise their goals.

In a study by Privacy International[8] many European states are not considered capable of upholding human rights standards on privacy. Only Greece is considered to have significant protection and safeguards. The Netherlands'

---

[6] Article 12 of the Council of Europe Convention on the Prevention of Terrorism, Warsaw, 2005 http://conventions.coe.int/Treaty/en/Treaties/Html/196.htm (accessed on 31 August 2009); also, see second paragraph: "The establishment, implementation and application of the criminalisation under Articles 5 to 7 and 9 of this Convention should furthermore be subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, and should exclude any form of arbitrariness or discriminatory or racist treatment."

[7] Translated from Dutch "Al weten wij de reden niet 't Is vast op goeden grond geschied.", Report, Commissie Datastromenen Veiligheid, August 2007, citing A.C.W. Staring, *De Hoofdige Boer*, 1820), Gegevensbestanden voor veiligheid: observaties en analyse. Rapport van de Adviescommissie Informatiestromen Veiligheid, NCTb, 2007, p.25.

[8] 'Leading surveillance societies in the EU and the World 2007', 28 December 2007. www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 (accessed on 31 August 2009).

Minister of Justice, Hirsch Ballin, stated on 30 November 2007 that security and privacy are equally codified in Articles 5 and 8 of the ECHR, not being absolute rights, but open to interference of authorities when needed.[9]

The effect of (terrorist) cybercrime can span the globe and one could argue that therefore harsher measures and extended competences have become a necessity. The complexity, and thus the difficulty in defining 'new criminal acts', may stand in the way of providing a clear description of the criminal conduct, its effects, and the (number of) perpetrators.

As stated by Ulrich Sieber:

> "The new risks are combined with a high complexity of offences that do not rest on technical or scientifical causes, but on specific perpetrator structures, a high number of victims or a high geographical expansion and extensiveness of the perpetration of the crime."[10]

Considering the subject of, electronic (supported) crime, national security and the instruments for investigation, one could conclude that there is no clear distinction between criminal acts, criminals and other (connected) persons. How should we apply criminal law under such circumstances? Sieber speaks of the "delimitation of criminal law and new security law", a dangerous development for the enforcement of fundamental human rights, in particular privacy.

## IV. Temptation for Authorities

The large quantity of personal data is a valuable resource for private and public entities. Private parties and public parties have different aims: enhancing profit, reducing costs, or making processing of all data more efficient by profiling techniques. For instance, many parties including physicians, hospitals, insurance companies and governmental health authorities may reap considerable financial benefit from the access to medical records data bases (e-health records).

Alternatively, protection of fundamental rights including the preservation of the integrity of personal life, and protection of personal information as an unalienable right for individuals, can also be considered to be important governmental goals. Therefore the validity and maintenance of informational and personal sovereignty as a fundamental right of civilians must be weighed against the interests that are pursued by state authority. The role of governmental authorities is, to say the least, ambivalent in this respect. There is a positive obligation of the governments to protect the rights of the

---

[9] http://www.justitie.nl/actueel/toespraken/archief-2007/71101privacy.aspx?cp=34&cs=581
(accessed on 31 August 2009).

[10] U. Sieber, 'Grenzen des Strafrechts', *Zeitschrift für die Gesamte Strafrechtswissenschaft* (119), May 2007, p.25.

individuals within the community and the negative obligation to respect those rights by not interfering.

This seems to be difficult for state authorities. The availability of personal data is almost seen as an invitation to use this data. However, the fundamental principles of human rights, as stated in international treaties and integrated in national law, should not be easily set aside for reasons that seem to be an exception on the merits of informational self-determination. Although, as stated by Bodin, there are circumstances in which certain rights may be set aside by the sovereign state, this must never be in contradiction with a just interpretation of (natural) laws or the result of unjust balancing of interests. This is the problem with which we are confronted.

What is the right balance between the fundamental principle of informational privacy and the general interest that allows derangement from this, based on the exceptions given in international and derived national law? Which circumstances allow state authorities to override fundamental principles? And, is there a difference in 'fundamentality' of human rights in this perspective?

Fundamental rights as protection against torture or slavery can be deemed absolute, but privacy is a right that, in practice, is considered less fundamental weighed against actions by the state. An interesting comparison can be made with the view of Westin in 1970 on the aspect of the surveillance state as characterisation of the modern totalitarian regime:

"The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups".[11]

Privacy is viewed as a kind of individualism that is considered antisocial behaviour.

## V. Balancing Privacy and Security

There must be scrutiny on merits based on fundamental human rights, the rights of other individuals, and non-discrimination in the sense of *summum jus summa injuria* : what seems to be equal is not always equal. These exceptions must be tested against the principles of protecting the informational sovereignty of individuals and the necessity to limit this fundamental right in light of the measures that have been taken by governmental authorities relating to the purpose they want to attain. Important in this view is the interpretation of the contextual interrelationship, practical concordance or *Ordnungszusammenhang*[12] in this task of balancing (individual) fundamental rights and community interests.

---

[11] *Idem*, p. 23, citing Margaret Mead.

[12] K. Hesse, *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, Heidelberg: C.F. Müller, 1995, 20th ed., no. 72 and 317 *et seq*. Cited and translated by T. Marauhn & N.

## VI. Discussion of the Dutch 'Passport Act'

A clear example of the shifting balance can be found in the new text of the Dutch 'Passport Act'[13], concerning the storage use and processing of biometric data. The Dutch senate agreed upon the text without many objections. This law is based on the European Council Regulation of 2004 ('the Regulation').[14] In the 1970's, a mass protection against the *'volkstelling'* census because of privacy concerns was still viable, keeping in mind the use of personal data by the Germans in the Second World War. In addition, there was the fear of 'automatisation' as such; what would the government do with all these data and how could a civilian ever control the processing of these data? In parliament and the senate there was not much discussion about the proposals to create a biometric passport based on the Regulation.[15] However, it is surprising that the Dutch law is going further than the Regulation. The purpose of the Regulation is solely to verify the authenticity of the document and the identity of the holder, although a more extensive use by government is not forbidden as such[16]. But the Dutch government saw an opportunity to extend the use of the change that the Regulation brought. They added an article in which the purpose of the biometric passport was much broader: these data could be used for criminal investigations and/or for researching activities that could form a threat against the security of the state and other important interests of the Netherlands or friendly nations. Further, it was determined that all these data should be stored in a data bank available for non-defined public purposes by police and intelligence agencies, without any clear legal limitation for use. Germany has strongly denied this central storage for security reasons. But other countries such as Belgium, France and Greece are moving towards the central data storage and use for public purposes.

## Conclusion

Threats on the security of countries must countered as much as possible, but not by all means. The use of personal data by investigative authorities must be closely monitored. Criminal law is the most intrusive law in society and must be handled with the utmost scrutiny by authorities. Treatment of the

---

Ruppel, *Balancing conflicting Human Rights: Konrad Hesse's notion of "Praktische Konkordanz"and the German Federal Constitutional Court*, in Eva Brems, p. 273 *et seq*.

[13] Eerste Kamer, 2008-2009, nr. 31324 (R1844)

[14] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. *Official Journal* L 385, 29 December 2004, pp. 1 – 6.

[15] See (in Dutch): http://www.eerstekamer.nl/behandeling/20090120/gewijzigd_voorstel_van_rijkswet/f=/vi21me9crbmv.pdf (accessed on 31 August 2009)

[16] Council Regulation (EC) No 2252/2004 (4) This Regulation is limited to the harmonisation of the security features including biometric identifiers for the passports and travel documents of the Member States. The designation of the authorities and bodies authorised to have access to the data contained in the storage medium of documents is a matter of national legislation, subject to any relevant provisions of Community law, European Union law or international agreements.

privacy of data subjects should be proportionate to a real threat to the interest of society and not based on fear. The seriousness of the crime and the phase of the process where these data are handled must be taken into consideration. The fundamental right of privacy must be handled with care. It is an obligation of the government to protect this principle of the democratic society.